UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/436,135	11/09/1999	DAVID VAN GUNTER	200310	6185

7590 06/17/2005

LEYDIG VOIT & MAYER LTD
TWO PRUDENTIAL PLAZA
SUITE 4900
180 NORTH STETSON
CHICAGO, IL 606016780

EXAMINER	
SHIN, KYUNG H	

ART UNIT	PAPER NUMBER
2143	

DATE MAILED: 06/17/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/436,135	**Applicant(s)** GUNTER, DAVID VAN ET AL	
	Examiner Kyung H. Shin	**Art Unit** 2143	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 March 2005*.

2a)□ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. This action is responding to application papers filed 3/4/2005.

2. Claims **1 - 15** are pending. Claims **1, 3, 8, 12** have been presently presented. Independent claims are **1, 8**.

3. The text of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Response to Arguments

4. Applicant's arguments, filed 3/4/2005, with respect to the rejection(s)of claim(s) 1-15 have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of **Hardjono et al.**.

4.1 In reply to an obviousness rejection under 35 U.S.C. § 103, (applicant's remarks, page 8.) test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981). Furthermore, in response to applicant's arguments against the reference individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208

USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

4.2 Applicant's arguments have thus been fully considered but in response to Applicant's arguments, 37 CFR § 1.111(c) requires applicant to "clearly point out the patentable novelty which he or she thinks the claims present in view of the state of the art disclosed by the references cited or the objections made."

Claim Rejections - 35 USC § 103

5. **Claims 1, 3, 4, 10, 11** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Jain et al.** (US Patent No. 6,311,218) in view of **Hardjono et al.** (US Patent No. 6,725,276).

Regarding Claim 1 (Previously Presented), Jain discloses a computer-readable medium having computer-executable instructions for operating a policy agent of a network for performing steps comprising:

a) detecting a network connection from a client computer on the network; (see Jain col. 4, lines 54-57: detect a network port connection)

b) composing a challenge for authenticating a user of the client computer associated with said network connection, the challenge being encrypted with a private key of the policy agent; (see Jain col. 2, lines 44-47: challenge-response authentication mechanism utilized)

c) transmitting the challenge to the client computer; (see Jain col. 2, lines 44-47: challenge presented to user)

d) receiving a response from the client computer; (see Jain col. 2, lines 44-47: response received)

e) decrypting the response using a public key of the user to obtain a first message digest value; (see Jain col. 6, lines 13-15: decrypt the response with public key)

Jain discloses a policy agent for network security. Jain does not disclose generation of a message digest from challenge and input (i.e. network) data. Jain does not disclose the comparison of a first and second message digest values to determine a match. Jain does not disclose processing of network data through a network connection to determine a match. However, Hardjono discloses:

g) the usage of a data message (i.e. network data, non-authentication information) plus key (i.e. authentication) information in the generation of a hash (i.e. digest), which is "used in an authentication scheme" (Remarks dated: March 1, 2005, Page 8, lines 2-2) and the determination of calculating a second message digest value based on the challenge and input (i.e. network) data; (see Hardjono col. 5, lines 20-30; col. 5, lines 30-35: authentication scheme utilizing key (i.e. authentication) data and message (i.e. non-authentication) data)

h) comparing the first and second message digest values to determine whether a match is found; (see Hardjono col. 5, lines 30-35: comparison of hash (i.e. digest) values to determine a match condition)

f) receiving network data through the network connection with the client computer; (see Hardjono col. 5, lines 20-30; col. 5, lines 30-35: authentication scheme utilizing key (i.e. authentication) data and message (i.e. non-authentication) data, comparison of hash (i.e. digest) values, forward data if a match)

i) if a match is found, then forwarding the network data to their specified recipient, else not forwarding the network data to their specified recipient. (see Hardjono col. 5, lines 20-30; col. 5, lines 30-35: authentication scheme utilizing key (i.e. authentication) data and message (i.e. non-authentication) data, comparison of hash (i.e. digest) values and forward data if a match)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Jain to utilize hash (i.e. message digest) generations and comparison within an authentication scheme as taught by Hardjono. One of ordinary skill in the art would be motivated to employ Hardjono in order to confirm the authenticity of transmitted and received messages for network communications. (see Hardjono col. 4, lines 25-28; col. 4, lines 30-33: “ *... confirm the authenticity of messages transmitted from the second multicast domain to the first multicast domain ... appending one or more authentication tags to the messages ... examine the authentication tags, if any, to confirm the authenticity of received messages ...* “)

Regarding Claims 3 (Previously Presented), **10** (Original), Jain discloses a computer-readable medium as in claims 1, 8, wherein the step of composing includes encrypting the challenge with a public key of the user. (see Jain col. 6, lines 2-9: encrypt challenge with public key)

Regarding Claims 4 (Original), **11** (Original), Jain discloses a computer-readable medium as in claims 3, 8, wherein the step of decrypting includes decrypting the response with a private key of the policy agent. (see Jain col. 6, line 2-9: decrypt response with private key)

6. **Claims 2, 6 - 9, 13, 15** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Jain-Hardjono** as applied to claim 1 above, and further in view of **Wesinger et al.** (US Patent No. 6,052,788).

Regarding Claim 2 (Original), Wesinger discloses a computer-readable medium as in claim 1, wherein the policy agent is a firewall. (see Wesinger col. 3, lines 55-57: policy agent, a firewall)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Jain to utilize a firewall as a data filtering mechanism as taught by Wesinger. One of ordinary skill in the art would be motivated to employ Wesinger in order to strengthen security for communications in network environments. (see Wesinger col. 3, lines 55-57: " *... provides a firewall that achieves maximum network security and maximum user convenience ...* ")

Regarding Claims 6 (Original), **13** (Original), Jain discloses an authentication mechanism utilizing cryptography, message digest generation and comparison. Jain does not disclose an out-of-band authentication mechanism utilizing network data packet filtering. However, Wesinger discloses a computer-readable medium as in claims 1, 8, wherein utilizing an out-of-band authentication mechanism and data filtering based on a pre-selected number of packets of the received network data (see Wesinger col. 4, lines 1-5; col. 10, lines 58-66: out-of-band authentication and network data packet filtering mechanism utilized), and Hardjono discloses the received network data are in the form of packets, and the step of calculating the second message digest value. (see Hardjono col. 5, lines 20-30; col. 5, lines 30-35: authentication scheme utilizing key (i.e. authentication) data and message (i.e. non-authentication) data, comparison of hash (i.e. digest) values and forward data if a match)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Jain to utilize an out-of-band authentication and data packet filtering mechanism as taught by Wesinger, and to utilize hash (i.e. message digest) generations and comparison within an authentication scheme as taught by Hardjono. One of ordinary skill in the art would be motivated to employ Wesinger in order to strengthen security for communications in network environments (see Wesinger col. 3, lines 55-57), and to employ Hardjono in order to confirm the authenticity of transmitted and received messages for network communications. (see Hardjono col. 4, lines 25-28; col. 4, lines 30-33)

Regarding Claims 7 (Original), **9** (Original), Jain discloses an authentication mechanism utilizing cryptography, message digest generation and comparison. Jain does not disclose an out-of-band authentication mechanism utilizing network data packet filtering. However, Wesinger discloses a computer-readable medium as in claims 1, 8, having further computer-executable instructions for performing an out-of-band authentication mechanism utilizing data packet filtering network access policies (see Wesinger col. 4, lines 1-5; col. 10, lines 58-66: out-of-band authentication and network data packet filtering encryption/decryption mechanism utilized), and Hardjono discloses wherein filtering the received network data according to the identity of the user after a match between the first and second message digest values is found. (see Hardjono col. 5, lines 20-30; col. 5, lines 30-35: authentication scheme utilizing key (i.e. authentication) data and message (i.e. non-authentication) data, comparison of hash (i.e. digest) values and forward data if a match)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Jain to utilize an out-of-band authentication and data packet filtering mechanism as taught by Wesinger, and to utilize hash (i.e. message digest) generations and comparison within an authentication scheme as taught by Hardjono. One of ordinary skill in the art would be motivated to employ Wesinger in order to strengthen security for communications in network environments (see Wesinger col. 3, lines 55-57), and to employ Hardjono in order to confirm the authenticity of transmitted and received messages for network communications. (see Hardjono col. 4, lines 25-28; col. 4, lines 30-33)

Regarding Claim 8 (Previously Presented), Jain discloses a method of authenticating a user using a client computer on a network to transmit network data through a policy agent of the network, comprising the steps of:

a) detecting by the policy agent a network connection from the client computer for transmitting network data of the user; (see Jain col. 4, lines 54-57: detect network port connection)

b) receiving by the policy agent network data transmitted through the network connection from the client computer; (see Jain col. 2, lines 55-58: receive data over network connection)

c) obtaining, by the policy agent, an identity of the user and a public key of the user; (see Jain col. 4, lines 27-36: obtain user identity)

d) composing, by the policy agent, a challenge encrypted with a private key of the policy agent; (see Jain col. 2, lines 44-47: challenge-response authentication mechanism utilized)

e) sending the challenge to the client computer; (see Jain col. 2, lines 44-47)

f) decrypting, by the client computer, the challenge; (see Jain col. 6, lines 13-15)

h) encrypting, by the client computer, the first message digest value with a private key of the user to create a response; (see Jain col. 5, line 66 - col. 6, line 2)

i) sending the response to the policy agent; (see Jain col. 6, lines 2-9)

j) decrypting, by the policy agent, the response to obtain the first message digest value; (see Jain col. 6, lines 13-15)

Jain discloses a policy agent for network security and using a out-of-band challenge authentication mechanism and network packet filtering system. Jain does not disclose generating a hash (i.e. message digest) utilizing input (i.e. network) data. Jain does not disclose the comparison of a first and second message digest values to determine a match. However, Hardjono discloses

k) calculating a second message digest value based on the challenge and network data received through network connections from the client computer; (see Hardjono col. 5, lines 20-30; col. 5, lines 30-35: authentication scheme utilizing key (i.e. authentication) data and message (i.e. non-authentication) data, comparison of hash (i.e. digest) values, forward data if a match)

l) comparing the first and second message digest values to determine whether there is a match, (see Hardjono col. 5, lines 20-30; col. 5, lines 30-35: authentication scheme utilizing key (i.e. authentication) data and message (i.e. non-authentication) data, comparison of hash (i.e. digest) values, forward data if a match)

g) generating, by the client computer, a first message digest value based on the network data of the user; (see Hardjono col. 5, lines 20-30; col. 5, lines 30-35: authentication scheme utilizing key (i.e. authentication) data and message (i.e. non-authentication) data, comparison of hash (i.e. digest) values, forward data if a match), and Wesinger discloses an out-of band authentication mechanism (see Wesinger col. 4, lines 1-5; col. 10, line 58-66: out-of-band authentication scheme)

m) wherein if a match is found, then forwarding, by the policy agent, the network data to their specified recipient, else not forwarding the network data to their specified recipient. (see Hardjono col. 5, lines 20-30; col. 5, lines 30-35: authentication scheme utilizing key (i.e. authentication) data and message (i.e. non-authentication) data, comparison of hash (i.e. digest) values, forward data if a match), and Wesinger discloses an out-of-band authentication and network filtering scheme (see Wesinger col. 4, lines 1-5; col. 10, line 58-66: out-of-band authentication, data filtering utilizing encryption and decryption)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Jain to utilize an out-of-band authentication and data packet filtering mechanism as taught by Wesinger, and to utilize hash (i.e. message digest) generation and comparisons within an authentication scheme as taught by Hardjono. One of ordinary skill in the art would be motivated to employ Wesinger in order to strengthen security for communications in network environments (see Wesinger col. 3, lines 55-57), and to employ Hardjono in order to confirm the authenticity of transmitted and received messages for network communications systems. (see Hardjono col. 4, lines 25-28; col. 4, lines 30-33)

Regarding Claim 15 (Original), Jain discloses a security server acting as a policy agent. Jain does not disclose a firewall. However, Wesinger discloses a method as in claim 8, wherein the policy agent is a firewall of the network. (see Wesinger col. 3, lines 55-57: policy agent, a firewall)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Jain to utilize an out-of-band authentication and data packet filtering mechanism as taught by Wesinger. One of ordinary skill in the art would be motivated to employ Wesinger in order to strengthen security for communications in network environments. (see Wesinger col. 3, lines 55-57)

7. **Claim 5** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Jain-Hardjono** as applied to claim 1 above, and further in view of **Goldman et al.** (US Patent No. 5,684,951).

Regarding Claim 5 (Original), Jain does not disclose generating a message digest with the inclusion of a time stamp. However, Goldman discloses a computer-readable medium as in claim 1, wherein the step of composing includes generating a message digest with the inclusion of a time stamp. (see Goldman col. 9, lines 34-41: generate message digest with timestamp value)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Jain to utilize message digest generation utilizing a time stamp value within an authentication system as taught by Goldman. One of ordinary skill in the art would be motivated to employ Goldman in order to strengthen security for network communications systems. (see Goldman col. 1, lines 60-66)

8. **Claims 12, 14** are rejected under 35 U.S.C. 103(a) as being unpatentable over

Jain-Hardjono-Wesinger as applied to claim 8 above, and further in view of **Goldman et al.** (US Patent No. 5,684,951).

Regarding Claim 12 (Original), Jain does not disclose generating a message digest with the inclusion of a time stamp. However, Goldman discloses a computer-readable medium as in claims 8, wherein the step of composing includes generating a message digest with the inclusion of a time stamp. (see Goldman col. 9, lines 34-41: generate message digest with timestamp value)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Jain to utilize message digest generation utilizing a time stamp value within an authentication system as taught by Goldman. One of ordinary skill in the art would be motivated to employ Goldman in order to strengthen security for network communications systems. (see Goldman col. 1, lines 60-66)

Regarding Claim 14 (Original), Jain discloses a challenge utilizing encryption/decryption techniques to enable an authentication challenge data decrypted from the challenge. Jain does not disclose the generation of a message digest utilizing random numbers. However, Goldman discloses a method as in claim 8, wherein the step of generating by the client computer generates the first message digest value based on a random number (see Goldman col. 9, lines 38-41: message digest generated utilizing random patterns, challenge (secret) and data), and Hardjono disclose wherein utilizing data of the pre-selected packets of the received network data.

(see Hardjono col. 5, lines 20-30; col. 5, lines 30-35: authentication scheme utilizing key (i.e. authentication) data and message (i.e. non-authentication) data, comparison of hash (i.e. digest) values, forward data if a match)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Jain to utilize hash (i.e. message digest) generation and comparisons within an authentication scheme as taught by Hardjono, and to utilize message digest generation utilizing a random number within an authentication mechanism as taught by Goldman. One of ordinary skill in the art would be motivated to employ Hardjono in order to confirm the authenticity of transmitted and received messages for network communications systems (see Hardjono col. 4, lines 25-28; col. 4, lines 30-33), and to employ Goldman in order to strengthen security for network communications systems (see Goldman col. 1, lines 60-66).

Conclusion

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kyung H. Shin whose telephone number is (571) 272-3920. The examiner can normally be reached on 9 am - 7 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David A. Wiley can be reached on (571) 272-3923. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KHS
Kyung H Shin
Patent Examiner
Art Unit 2143

KHS
June 11, 2005

WILLIAM C. VAUGHN, JR.
PRIMARY EXAMINER